ABSTRACT OF THE DISCLOSURE

A modular exponentiation calculation apparatus obtains a first RNS representation of a value $Cp^{dp} \times B \bmod p$ based on an RNS representation of a remainder value $Cp = C \bmod p$ and a remainder value $dp = d \bmod (p - 1)$, obtains a second RNS representation of a value $Cq^{dq} \times B \bmod q$ based on an RNS representation of a remainder value $Cq = C \bmod q$ and a remainder value $dq = d \bmod (p - 1)$, obtains a third RNS representation of an integer m′ congruent with $C^d \bmod (p \times q)$ based on both the first and second RNS representations, and obtains $m = C^d \bmod (p \times q)$ based on a value of the integer m′ obtained by converting the third RNS representation into a binary representation.